U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Secure Transport (ST) system
Bureau/Office: Office of the Chief Information Officer
Date: 4/21/2020
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

Secure Transport is a minor application hosted and managed by the Department of the Interior (DOI), Office of the Chief Information Officer (OCIO), Hosting Services Branch, Enterprise Services Division. Secure Transport is a web-based Transport Layer Security (TLS1.2 enforced) file transfer system that allows authorized users the ability to securely transfer files between DOI users, bureaus and offices, and internal or external customers either manually or via system scripted uploads and downloads.

Secure Transport is provided as-a-service within DOI and to external customers including Federal, state, tribal and local agencies, and private organizations. Secure Transport supports security functionalities to ensure connection level security, transport level security, folder/file level security and authentication security. Secure Transport customers retain ownership and control over their own records when using the service and are responsible for meeting requirements under the Privacy Act and other applicable laws and policies for the collection, maintenance, use, and sharing of their records within the system.

C. What is the legal authority?

5 U.S.C. 301, Departmental Regulations; 44 U.S.C. Chapter 35, The Paperwork Reduction Act; 40 U.S.C. 1401, the Clinger-Cohen Act of 1996.

D. Why is this PIA being completed or modified?

☒ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

UII Code: 010-000002507, Secure Transport System is a minor application hosted in the OCIO Data Center Boundary General Support System. A System Security and Privacy Plan is being developed for Secure Transport.

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☐ Yes: *List Privacy Act SORN Identifier(s)*
☒ No

Secure Transport is a file transfer system that allows the ability to securely transfer files between organizations and is not intended to be used as a record keeping system and does not require publication of a SORN. However, Active Directory network credentials are covered under DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040 (March 12, 2007), which is currently under revision. Customers retain ownership of their records transferred in Secure Transport and are responsible for meeting any notice requirements under the Privacy Act for the records under their control.

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Personal Cell Telephone Number
☒ Other: *Specify the PII collected.*

Secure Transport files that are uploaded or downloaded may contain numerous data types which may include all types of PII and other sensitive data, such as transfer of data between DOI and

auditors for defined audit events. Any customer user may request a Secure Transport account by contacting the OCIO Customer Support Center (CSC) Helpdesk and submitting a request through the DOI Remedy System, OCIO's help desk ticketing system. The Remedy System creates a ticket that includes the name of the requester, organization or customer company, contact information, customer site, and customer desk location. Secure Transport usernames consist of the user's business email address, and the usernames, passwords and users' business phone number are kept as a record within Secure Transport for the purpose of authenticating users. In some limited cases, external users may choose to use personal phone number or email address as their contact information. User data is encrypted and managed by System Administrators. Passwords cannot be viewed by System Administrators.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency
☒ Tribal agency
☒ Local agency
☒ DOI records
☒ Third party source
☒ State agency
☒ Other: *Describe*

Customers may be internal DOI bureaus and offices, other agencies, or organizations external to DOI. Customers contact the CSC Helpdesk to provide a user's name and contact information to request a user account to access Secure Transport. The CSC Helpdesk completes the Secure Transport user request form OCIO-26, Active Directory (AD) & Windows Elevated Privileges Request, through the DOI Remedy system to initiate creation of Secure Transport accounts. The OCIO-26 form includes customer name, phone number, email address, customer agency, company or organization, customer site, customer desk location, and other administrative information related to access roles necessary to complete the request.

The IT Windows Hosting staff may contact the customer via the customer supplied telephone number or email address to provide a username and instructions on accessing Secure Transport. IT Windows Hosting Team system administrators are required to authenticate to Windows servers via their DOI issued Personal Identity Verification (PIV) card, which is authenticated through the Enterprise Active Directory system.

C. How will the information be collected? Indicate all that apply.

☐ Paper Format
☐ Email

☐ Face-to-Face Contact
☒ Web site
☐ Fax
☒ Telephone Interview
☐ Information Shared Between Systems *Describe*
☒ Other: *Describe*

Requests for Secure Transport accounts and user access are processed via the CSC Helpdesk in the DOI Remedy System through the OCIO-26, Active Directory (AD) & Windows Elevated Privileges Request Form. Requests are managed as tickets within Remedy and automatically assigned to the IT Windows Hosting Team. Windows IT System Administrators manually access the Remedy system to view details of the ticket and verify with Secure Transport folder structure owners if the individual making the request is authorized to access the specified folder. Once verified, an IT Windows Hosting Team system administrator logs into Secure Transport, creates the username and assigns rights to requested folder structures. IT Windows Hosting staff contact the customer via customer supplied telephone number or email address to provide username and instructions on accessing Secure Transport.

Users access Secure Transport via website at https://securetransport.ibc.doi.gov/ and are presented with a Security Warning Banner on the login screen. Only authorized Secure Transport users can log into Secure Transport to access specific folders/files.

D. What is the intended use of the PII collected?

The purpose of the system is to ensure secure file sharing. User name and contact information are required to create and manage Secure Transport user accounts and authenticate users for security purposes to ensure the confidentiality of the records shared or transferred. User account data is used to identify individual users and manage access to specific folders and to notify users of any Secure Transport issue or scheduled maintenance.

Secure Transport users have authorized access to specific folders/files which may contain PII or sensitive data and have the ability to perform file uploads and downloads either manually or via system scripts. Authorized users log in to Secure Transport to upload, download or view their files, or to remove files. Files transferred through Secure Transport are automatically deleted after 15 days unless there is a waiver in place for them to remain longer.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*
User information may be shared with IT Windows System Administrators in the Hosting Services Branch, Enterprise Services Division on a need-to-know basis for account management

purposes. IT Windows System Administrators have elevated rights to access all folder structures in Secure Transport to ensure system operational oversight and policy enforcement. Secure Transport users have authorized access to specific folders/files which may contain PII or sensitive data and have the ability to share files within their organizations and perform file uploads and downloads either manually or via system scripts.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

Users will have access to files or folders explicitly authorized by the data owner. Ad-hoc reporting of Secure Transport bureau user email addresses and telephone numbers may be shared with specific bureaus and offices upon authorized request. Users cannot edit files in Secure Transport. Files are automatically deleted after 15 days unless there is a waiver in place for them to remain longer. Secure Transport is strictly for authorized file sharing purposes. Secure Transport users have the ability to share files with other organizations and perform file uploads and downloads either manually or via system scripts. Each bureau/office data owner is responsible for ensuring their data shared via Secure Transport is for authorized purposes only.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Secure Transport has numerous Federal agency customers such as the U.S. Department of Transportation, Federal Aviation Administration (FAA), and U.S. Department of the Treasury. Federal agency customers may be the recipients of files or data owners and have access to their own folders/files structures in Secure Transport, which may contain PII or sensitive data. Federal agency customers have the ability to perform file uploads and downloads, either manually or via system scripts, and to manage or remove files. Secure Transport is strictly for authorized file sharing purposes. Federal agency customer data in Secure Transport will only be shared at the request of the data owner for the specified timeframe. Users cannot edit files in Secure Transport. Files are automatically deleted after 15 days unless there is a waiver in place for them to remain longer. Federal agency customers using Secure Transport are the data owners of the contents of files they transfer via Security Transport and are responsible for ensuring their data is managed and shared in accordance with the Privacy Act and related laws and policies, and complying with the notice and access provisions of the Privacy Act.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Tribal, State or Local agencies may be customers or recipients of file sharing from DOI bureaus, offices or other customers through Secure Transport. These agencies may have access to their folders/files, which may contain PII or sensitive data, and have the ability to perform file uploads and downloads, either manually or via system scripts, and to manage or remove files. Folder owners are responsible for ensuring their data shared via Secure Transport is for authorized purposes only.

☒ Contractor: *Describe the contractor and how the data will be used.*

Information may be shared with DOI authorized contractor staff acting on behalf of DOI on a need-to-know basis in support of DOI activities related to administration and use of the system. OCIO has a maintenance contract with the Secure Transport vendor and may be required to perform online troubleshooting with the vendor to resolve an ongoing issue. The vendor does not have access to data within Secure Transport system folder structure.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

Private organizations using Secure Transport may have access to their folders/files, which may contain PII or sensitive data, and have the ability to perform file uploads and downloads either manually or via system scripts. Folder owners are responsible for ensuring their data is shared via Secure Transport is for authorized purposes only.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Users provide information to a DOI sponsor or customer organization who in turn provides it to the CSC Helpdesk to complete the OCIO-26 form in order to create user accounts to access Secure Transport. Users also voluntarily provide their contact information to the CSC Helpdesk when requesting Secure Transport accounts or requesting assistance with a Secure Transport issue. Secure Transport management is based on a secure folder structure with designated folder owners. Prior to assigning privileges to a Secure Transport folder structure, IT Windows System Administrators verify with the folder owner if the individual making the request is authorized to access the specified folder, if authorization is given, access is granted.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement: *Describe each applicable format.*

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided on the log in page. Notice is also provided to individuals through the publication of this privacy impact assessment.

☒ Other: *Describe each applicable format.*

The following warning banner is displayed on the Secure Transport Login page:

"WARNING TO USERS OF THIS SYSTEM THIS IS A NOTICE OF MONITORING OF THE DEPARTMENT OF THE INTERIOR (DOI) INFORMATION SYSTEM"

This computer system, including all related equipment, networks, and network devices (including Internet access), is provided by the Department of the Interior (DOI) in accordance with the agency policy for official use and limited personal use. All agency computer systems may be monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. **This system contains CUI**. Any information on this computer system may be examined, recorded, copied and used for authorized purposes at any time. All information, including personal information, placed or sent over this system may be monitored, and users of this system are reminded that such monitoring does occur. Therefore, there should be no expectation of privacy with respect to use of this system. By logging into this agency computer system, you acknowledge and consent to the monitoring of this system. Evidence of your use, authorized or unauthorized, collected during monitoring may be used for civil, criminal, administrative, or other adverse action. Unauthorized or illegal use may subject you to prosecution.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Secure Transport is a web-based file transfer system that allows authorized users the ability to securely transfer files either manually or via system scripted uploads and downloads. System Administrators may retrieve user account data by username or folder name.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

Reporting is not inherent within Secure Transport. IT Windows System Administrators have written a script which will create a Secure Transport username report that includes; Account Name, Email Address, who requested the account along with the Remedy ticket number, folder access and folder structure owner. The script is run on an ad-hoc basis only for account management and security purposes.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

User data is provided by DOI sponsors, customers and users to request access to Secure Transport and is presumed to be accurate at the time it is submitted. Incomplete or inaccurate data would result in inability to contact the user or create an account. User data may be verified with the data owner for security purposes. The review of data for file transfers and username accuracy is the responsibility of the customer communities. The Secure Transport customer base is responsible for authorizing all requests for action, to include establishing, changing and removing accounts and folders. IT Windows System Administration staff do not act without an authorized DOI Remedy system request. Without such notification, system administrators have no mechanism to know when a related user status, position, or inherit commitment changes. IT Windows System Administration staff perform a periodic review of Secure Transport accounts and any account that has not been accessed in 90-days is disabled.

B. How will data be checked for completeness?

User data is provided by DOI sponsors, customers and users to request access to Secure Transport and is presumed to be complete at the time it is submitted to the CSC Helpdesk. User data may be verified with the data owner for security purposes. The review of data to ensure data completeness is the responsibility of the customer communities. Incomplete data would result in inability to contact the user or create an account as IT Windows System Administration staff have no mechanism to check data completeness except to verify data with the sponsor or customer.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

User data is provided by DOI sponsors, customers and users to request access to Secure Transport and must be current at the time it is submitted to the CSC Helpdesk in order to create user accounts. User data may be verified with the data owner for security purposes. The review of user data for file transfers to ensure currency is the responsibility of the customer communities. IT Windows System Administration staff have no mechanism to ensure data is current except to verify data with the sponsor or customer.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

System user account records are maintained under Departmental Records Schedule (DRS) 1.4.0013 Short-term Information Technology Records, System Maintenance and Use Records, which is approved by the National Archives and Records Administration (NARA) (DAA-0048-2013-0001-0013). These records have a temporary disposition and are determined obsolete when they are no longer needed for administrative, legal, audit, or other operational purposes, and destroyed no later than 3 years after cut-off.

Secure Transport is not considered a file retention system, it is designed for files to be uploaded/downloaded to/from the folder structures. Customers, including DOI bureaus and offices, Federal, state or local agencies, and private organizations, using Secure Transport are the data owners of the contents of files transferred via Security Transport and are responsible for ensuring their data is appropriately managed in accordance with law and policy.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Secure Transport is not considered a file retention system, it is designed for files to be uploaded/downloaded to/from the folder structures. Approved disposition methods for DOI user records are in accordance with 384 Department Manual 1 and NARA guidelines.

IT Windows System Administration staff run nightly scripts that identify and remove files that have been on Secure Transport for a period of 15 days. Customers are responsible for ensuring files are uploaded/downloaded in a timely manner and for meeting any records management requirements under the Federal Records Act. Most Secure Transport user accounts are used yearly, each user account is assigned a license. Inactive users accounts are disabled and remain disabled until a ticket is submitted via Remedy to re-enable.

Customers may request a waiver to keep files on Secure Transport longer than 15 days. Waiver requests are submitted, approved and processed via the CSC Helpdesk. Waiver requests are created as incident tickets within Remedy to include customer waiver request details and are assigned to the IT Windows Hosting Team. Waiver request details are noted and stored in a "Waivers" folder in Secure Transport and are periodically reviewed.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a limited risk to individual privacy for use of the majority of user accounts as PII required to create a Secure Transport account is limited to customer name, customer agency or company, customer phone number and email address, customer site, and customer desk location, which are generally official information that is not considered as sensitive in nature. However, there is an increased privacy risk for any use of personal contact information, use of username and password, and for the data files transferred via Secure Transport as files may contain various

types of PII that may be sensitive and pose a risk to the privacy of individuals. Secure Transport requires strict security and privacy controls to protect the confidentiality, integrity, and availability of data in the system. The use of DOI Information Systems is conducted in accordance with the appropriate DOI Security and Privacy Control Standards policy and NIST guidelines.

There is a risk that unauthorized individuals may access, use or share data for unauthorized purposes. Secure Transport requires authentication via DOI's AD for internal users and an individual's username and password for external users and some internal users. Folder/file access is assigned to authorized users at the request of the folder owner. All user access is strictly controlled and user activity within Secure Transport is monitored for security purposes. Access must be specifically authorized by the folder owner in order to upload or download files by any other user. Additionally, only authorized users with the proper skill sets and "need-to-know" are given access to the system.

IT Windows System Administrators have elevated accounts (different than their least privileged user account that is used for every day functionality) that provides elevated access to all Windows Servers within the OCIO Hosting Environment. Requests for elevated accounts are processed via the CSC Helpdesk. Requests are created as incident tickets with Remedy, approved and assigned to the OCIO End User Administration Team for creation. All IT Windows System Administrators and users are required to take role-based training and sign DOI Rules of Behavior that identify the need to protect PII data prior to gaining access, and also must complete initial and annual Federal Information Systems Security Awareness (FISSA) and Privacy Awareness training. Failure to comply with DOI Rules of Behavior may result in disciplinary action for DOI employees. External customers are data owners and are responsible for ensuring the appropriate access and use of the files shared with other organizations.

There is a risk the data may be stored for longer than necessary in Secure Transport. Files are automatically deleted after 15 days unless there is a waiver in place for them to remain longer. Clients are allowed to request a waiver to keep files on Secure Transport longer than 15 days. Waiver requests are submitted, approved and processed via the CSC Helpdesk. Waiver requests are created as incident tickets within Remedy and assigned to the IT Windows Hosting Team. Customers are the data owners of the contents of files transferred via Security Transport and are responsible for the records under their ownership and control and ensuring their data is appropriately managed. Only minimal user data is collected and maintained to manage user accounts and user records are covered by a NARA approved records retention schedule.

There is a risk that folders/files that contain PII or sensitive data can be inappropriately accessed during file transfer or when stored on Secure Transport. Secure Transport is undergoing the Assessment and Authorization process and has a moderate security categorization in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. A system security and privacy plan is being developed to identify controls implemented or planned to ensure appropriate safeguards are in

place. Secure Transport is hosted in a secure DOI facility and is protected by physical controls, firewalls, network security configurations, and other security protocols to strictly control user access and use, and ensure the confidentiality of the data in the system. System administrators and other authorized roles are based on least privilege principles. User access is monitored and audited to ensure the security of the system and data in accordance with Federal laws and DOI security and privacy policy.

Secure Transport is designed to allow secure, reliable, easy to use manual file transfer or system scripted transfer capabilities, and supports security functionality to ensure connection level security, transport level security, folder/file level security and authentication security. TLS encryption, and Public Key Infrastructure (PKI) certificates are enforced. Folder/file access are assigned to authorized users to ensure auditable activities. Files/folders are encrypted using FIPS 140-2 compliant algorithms both at rest and in transit. An audit log is configured on Secure Transport to track configuration changes. In addition, auditing is configured on the Operating System of the Windows Server. Secure Transport is part of the monthly security vulnerability scan process and any identified vulnerabilities are noted and addressed.

There is a risk that individuals may not receive adequate notice on how their data will be used or shared. A Privacy Notice is provided on the log in page. Notice is also provided through publication of this privacy impact assessment, which informs individuals on how user data is managed, how their login credentials are obtained, shared, stored, and managed in order to obtain access, and how files are securely shared in the Secure Transport system. Any additional notice to individuals required by law and policy for specific sharing of records that contain PII with other organizations is the responsibility of the customer who is the data owner.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

Secure Transport is a web-based file transfer system allowing authorized users the ability to securely transfer files either manually or via system scripted uploads and downloads. PII collected is used for account management purposes.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*

☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*

☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☐ Other: *Describe*

Users: Users are internal and external customers and recipients of file sharing. Users only have access to assigned folders/files as requested by data owners. Requests for Secure Transport accounts and access are processed via the CSC Helpdesk, OCIO-26 form in the DOI Remedy System. Requests are created as incident tickets within Remedy and automatically assigned to the IT Windows Hosting Team. Windows IT System Administrators manually access Remedy system to view details of the incident ticket and to verify with Secure Transport folder structure owners if the individual making the request is authorized to access the specified folder. Once verified, an IT Windows Hosting Team system administrator logs into Secure Transport, creates the username and assigns rights to requested folder structures. IT Windows Hosting staff contact the customer via customer supplied telephone number or email address to provide username and instructions on accessing Secure Transport.

System Administrators: All IT Windows System Administrators have elevated accounts (different than their least privileged user account that is used for every day functionality) that provides elevated access to all Windows Servers within the OCIO Hosting Environment. Requests for elevated accounts are processed via the CSC Helpdesk. Requests are created as incident tickets with Remedy, approved and assigned to the OCIO End User Administration Team for creation. IT Windows Hosting Team system administrators are required to authenticate to Windows servers via their DOI issued PIV card.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Secure Transport user accounts and access to folders/files are strictly controlled. Any request for an account is processed via the OCIO-26 form, which requires a sponsor and supervisory approval and a IT Windows Team lead approval. Any request for access to folders/files are approved by the folder/file owner prior to access is given. The purpose of Secure Transport is to provide a secure file transfer mechanism to OCIO, DOI, non-DOI and sponsored general public customers supported by OCIO – Hosting Services Branch, Enterprise Services Division.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Privacy Act clauses were inserted into the vendor contract.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

An audit log is configured on Secure Transport to track configuration changes. In addition, auditing is configured on the Operating System of the Windows Server. Secure Transport is part of the monthly security scan process and any identified vulnerabilities are noted and addressed.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

Secure Transport is configured to monitor the activities of users based on their username. Activities monitored are login date/time, failed logins, file transfer activity, and file deletion activities.

M. What controls will be used to prevent unauthorized monitoring?

Only IT Windows System Administrators are authorized to view Secure Transport audit logs. Secure Transport user accounts and access to folders/files are strictly controlled. Audit logs are used to monitor user activity for security purposes. Any request for an account is process via the OCIO-26 form, which requires a supervisory approval and an IT Windows Team lead approval. Any request for access to folders/files are approved by the folder/file owner prior to granting access. IT Windows System Administrators sign DOI Rules of Behavior that identify the need to protect PII data prior to gaining access, and also must complete initial and annual Federal Information Systems Security Awareness (FISSA) and Privacy Awareness training. Failure of DOI employees to comply with DOI Rules of Behavior may result in disciplinary action.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television

☐ Cipher Locks
☒ Identification Badges
☒ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☐ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Secure Transport Information System Owner is responsible for oversight and management of security and privacy controls and ensuring the protection of data within the system. The Secure Transport System Owner and the Information System Security Officer are responsible for ensuring adequate safeguards are implemented in compliance with Federal laws and policies.

The Information System Security Officer is responsible for continuous monitoring of security controls and ensuring the Information System Owner is informed of any issues or complaints. Internal and external customers and authorized users are responsible for using the Secure Transport in accordance with Federal law and policy and DOI requirements.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The Secure Transport Information System Owner is responsible for daily operational oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The Information System Owner, Information System Security Officer, and authorized users of the Secure Transport system are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals, in consultation with DOI Privacy Officials and data owners.